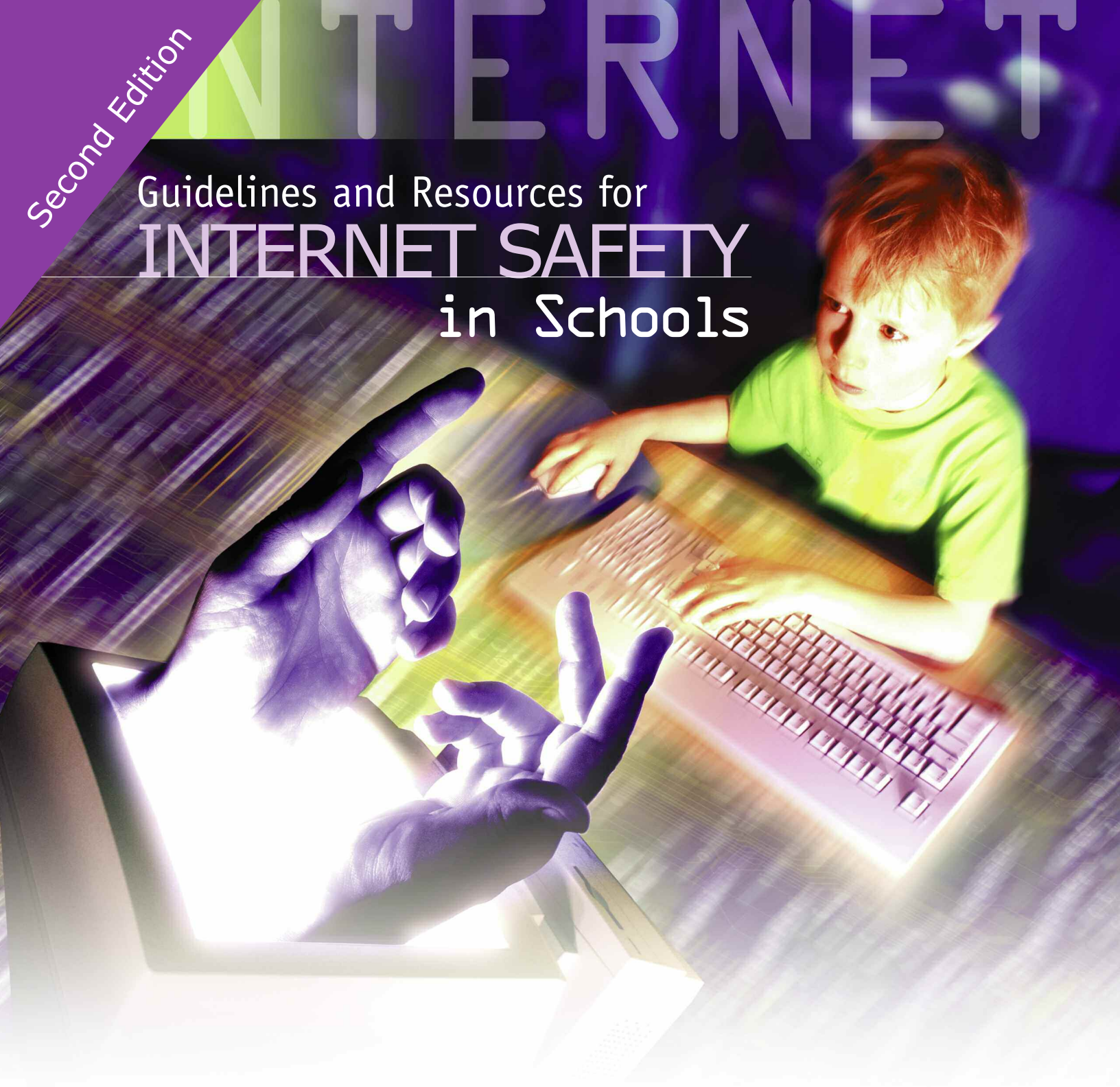


Second Edition

# INTERNET

## Guidelines and Resources for INTERNET SAFETY in Schools



VIRGINIA DEPARTMENT OF EDUCATION  
DIVISION OF  
**TECHNOLOGY &  
CAREER EDUCATION**  
OFFICE OF EDUCATIONAL TECHNOLOGY

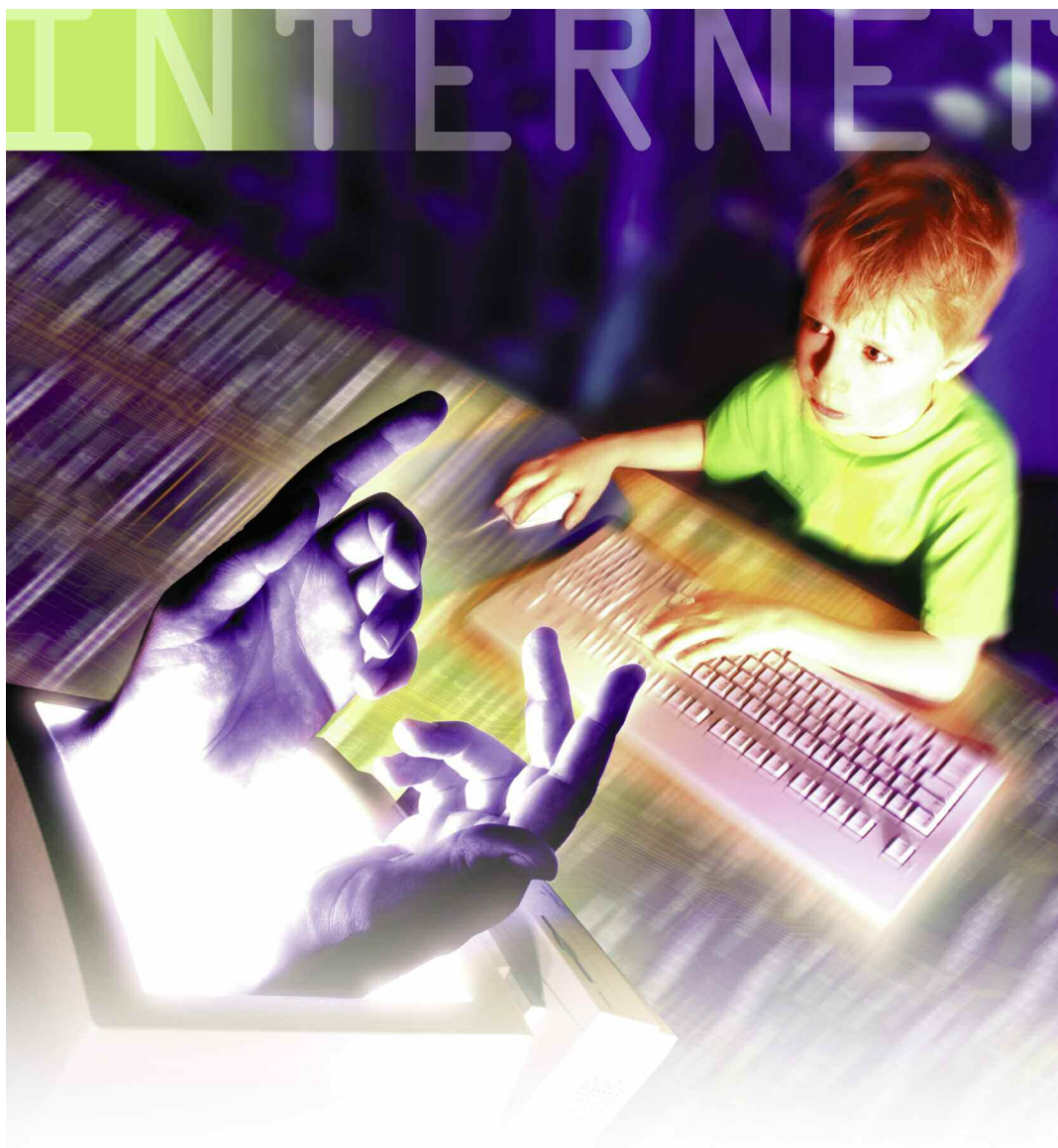
**OCTOBER 2007**

Guidelines and Resources Developed in Response  
to Chapter 52 – An Act to Amend and Reenact  
§ 22.1-70.2 of the *Code of Virginia*, Relating to  
Internet Safety Instruction in Schools  
(HB58 – Approved March 7, 2006)

***Disclaimer***

This document provides links to Web sites created and maintained by other public and/or private organizations. The Virginia Department of Education provides links to these sites for information purposes only; the presence of a link is not an endorsement of the site. Although every reasonable effort is made to present current and accurate information, Internet content appears, disappears, and changes over time. Please let us know about existing external links that might be inappropriate.

# Guidelines and Resources for INTERNET SAFETY in Schools



VIRGINIA DEPARTMENT OF EDUCATION  
DIVISION OF  
**TECHNOLOGY &  
CAREER EDUCATION**  
OFFICE OF EDUCATIONAL TECHNOLOGY

First Edition, September 2006  
Second Edition, October 2007



# Guidelines and Resources for Internet Safety in Schools

## *State Board of Education*

Dr. Mark E. Emblidge, President  
Dr. Ella P. Ward, Vice President  
Dr. Thomas M. Brewster  
Isis M. Castro  
David L. Johnson  
Dr. Gary L. Jones  
Kelvin L. Moore  
Andrew J. Rotherham  
Eleanor B. Saslaw

## *Virginia Department of Education*

Dr. Billy K. Cannaday, Jr.  
Superintendent of Public Instruction

### *Division of Technology*

Lan Neugent  
Assistant Superintendent

### *Office of Educational Technology*

Dr. Tammy McGraw  
Director



# Contents

Acknowledgments .....	iv
Foreword .....	v
Introduction .....	1
Legislation .....	2
Issues School Divisions Must Address .....	4
Integrating Internet Safety into Curriculum Content Instruction .....	6
What Students Need to Know .....	7
What Parents, Grandparents, and Caregivers Need to Know .....	10
What Teachers, Instructional Technology Resource Teachers, Library Media Specialists, Counselors, and Resource Officers Need to Know .....	13
What School Administrators Need to Know .....	16
What School Boards Need to Know .....	18
Appendixes	
A. Legislative Act, Chapter 52 .....	20
B. SUPTS. MEMO NO. 15, April 21, 2006 .....	21
C. Internet Safety and the Virginia Standards of Learning for Computer/ Technology for Grades K-12 .....	22
D. Web-Based Resources on Internet Safety .....	24
E. Glossary .....	45



# Acknowledgments

Marcie Altice, Franklin County Public Schools  
Jon Bernstein, Bernstein Strategy Group  
Donna Bowman, Virginia Center for School Safety, Department of Criminal Justice Services  
Donnie Brooks, Southwest Virginia Governor's School for Science, Mathematics, and Technology  
Michael J. Brown, Sheriff of Bedford County, Virginia  
Dr. James Carroll, Arlington Public Schools  
Dr. Chris Corallo, Henrico County Public Schools  
Cheryl Elliott, James Madison University  
Dr. Ann Flynn, National School Boards Association  
Delegate William H. Fralin, Jr., Virginia General Assembly  
Patricia Greenfield, Department of Psychology and Children's Media Center, UCLA  
Jim Lantzy, George Mason University  
Charlie Makela, Arlington Public Schools  
Roxanne Mills, Virginia Educational Media Association  
Susan Patrick, North American Council for Online Learning  
Dr. Gary Reynolds, Project Blue Ridge Thunder, Bedford County Sheriff's Office  
Teri Schroeder, iSafe  
Joe Showker, Rockingham County Public Schools  
Michele Stockwell, Education, Social and Family Policy, Progressive Policy Institute  
Ron Teixeira, National Cyber Security Alliance  
Lisa M. Hicks-Thomas, Computer Crimes Unit, Office of the Attorney General  
George F. Washington, Franklin County Public Schools  
Dr. John R. Wenrich, Institute for Connecting Science Research to the Classroom, Virginia Tech  
Nathaniel C. Wood, Division of Consumer and Business Education, Federal Trade Commission  
Dr. Zheng Yan, University of Albany

## *Virginia Department of Education*

Gloria Barber (Retired)  
Betsy Barton  
Stan Bumgardner  
Arlene Cundiff  
Michael Fleshman  
Caroline Fuller  
Dr. Tammy McGraw  
Sara Marchio  
Lan Neugent  
Penny Robertson  
Anne Rowe  
Michelle Vucci  
Greg Weisiger  
Jean Weller  
Anne Wescott  
Joyce Faye White



## Foreword

Today's students will be the first generation to use the Internet for their entire lives. This unprecedented access to resources will enhance their learning, research, communications, explorations for new ideas, and expressions of creativity. Unfortunately, this remarkable resource has become susceptible to abuse that often targets young people.

The Virginia Department of Education is committed to helping school divisions develop and implement Internet safety policies and programs, as directed by HB58. This document, *Guidelines and Resources for Internet Safety in Schools*, provides a starting point as divisions add required Internet safety components to their acceptable use policies. The legislation also compels divisions to integrate Internet safety into their curricula. While the document offers recommendations, specific curricular details are left to the discretion of school systems.

The Department developed these guidelines with input from individuals and organizations throughout the Commonwealth and beyond. It represents the knowledge and perspectives of educators; researchers; law enforcement officials; local, state, and federal representatives; and independent nonprofit organizations. The Department will periodically disseminate additional information and resources, beginning with a fall 2006 document that demonstrates how Internet safety issues can be integrated with the Standards of Learning.

As educators, perhaps our greatest priority is to protect the students. In terms of online safety, the ever-changing nature of the Internet makes this objective a constantly moving target. Although the task is daunting, we must stay ahead of the curve in detecting and reporting Internet threats and predators. Instructors need to be well-informed about the latest computer threats and integrate Internet safety into their curricula throughout the school year. Administrators should keep staff and community members apprised of new developments. They also need to evaluate the Internet safety program's quality and effectiveness and make regular adjustments and revisions.

As you develop and later evaluate Internet safety policies and programs, I encourage you to share best practices and successes with the Department's Office of Educational Technology. Questions about *Guidelines and Resources for Internet Safety in Schools* also should be directed to the office at 804-225-2855.

The Internet's potential is limitless and still largely untapped. Within the next 10 years, it will change education in ways we never could have imagined. My goal is for the Commonwealth of Virginia to remain a national leader in educational technology by pioneering cutting-edge uses of the Internet while ensuring the safety of each student.

Billy K. Cannaday, Jr.  
Superintendent of Public Instruction





## Introduction

Few would argue that the Internet has had a profound influence on education, including an unprecedented access to resources, opportunities for collaboration across geographic and temporal barriers, and engagement in global communities. Current research suggests this impact may extend to student academic achievement. In a recent study of low-income students, Linda Jackson and her colleagues at Michigan State University found that increased Internet use correlates with higher standardized reading-achievement scores and grade-point averages.<sup>1</sup>

The high-speed Internet has made the Web much more interactive, with communication possibilities expanded beyond the written word. While young people tend to adopt new technologies more quickly than adults, many do not have the experience or knowledge to understand the potential risks. Parents, educators, and community members must encourage students to take advantage of the Internet's benefits while reducing its risks.

All Virginia school divisions currently have Internet acceptable use policies and employ filtering software. These policies and filters are necessary but cannot prevent all risks to students. Since Internet threats change constantly, schools and divisions must take additional steps to safeguard students.

The Virginia Department of Education has published *Guidelines and Resources for Internet Safety in Schools* to assist school divisions in three areas: (1) writing an Internet safety component as part of the acceptable use policy, (2) integrating Internet safety into the curriculum, and (3) fostering responsibility among all stakeholders to help protect young people from online dangers. This document also will explain the meanings of new terms commonly used in cyberspace. Words italicized in the text are explained in more detail in the Appendix E glossary.

Additional information about Internet safety may be found on the Department's Web site at <http://www.doe.virginia.gov/VDOE/Technology/OET/internet-safety-guidelines.shtml>.

---

<sup>1</sup>L. A. Jackson, A. von Eye, F. A. Biocca, G. Barbatsis, Y. Zhao, and H. E. Fitzgerald, "Does home Internet use influence the academic performance of low-income children?" *Developmental Psychology*, 42(3):1-7 (2006).



## Legislation

The Virginia General Assembly proactively has promoted the Internet's instructional benefits while protecting students from its risks. In 2000, a state law required school divisions to develop acceptable use policies, which provide Internet guidelines for students and teachers. The following year, state and federal laws authorized the installation of filtering software to prevent students from accessing potentially harmful material.

House Bill 58, introduced by Delegate William H. Fralin, Jr., and passed by the 2006 General Assembly, requires that school divisions' acceptable use policies "include a component on Internet safety for students that is integrated in a division's instructional program." The legislation also requires the Superintendent of Public Instruction to issue guidelines to school divisions regarding instructional programs related to Internet safety. For the new legislation, see the italicized sections in Section A of Appendix A.<sup>2</sup> The acting superintendent of public instruction issued a memorandum regarding the legislation and requirements (see Appendix B).<sup>3</sup>

The revised policy must comply with current federal, state, and local laws relating to Internet safety:

- **Acceptable Use Policies (AUP) for Public and Private Schools (*Code of Virginia § 22.1-70.2*).** This law reflects the circumstances unique to the school or division and the electronic system used; it clearly defines responsible use of information networks.
- **Family Involvement in Technology (FIT) Program (*Code of Virginia § 22.1-212.2:3*).** This program promotes parental and family involvement in children's education, including increased and appropriate supervision of children using the Internet.
- **Children's Internet Protection Act (CIPA).** Congress enacted this law in December 2000 to address offensive Internet content on school and library computers. It imposes specific requirements on any school or library that receives funding support for Internet access or internal connections from the E-Rate Program.<sup>4</sup>

---

<sup>2</sup>The text of the legislation also is available at <http://leg1.state.va.us/cgi-bin/legp504.exe?ses=061&typ=bil&val=hb58> [12 August 2006]

<sup>3</sup>A copy of the memorandum also is available at <http://www.doe.virginia.gov/VDOE/suptsmemos/2006/adm015.html> [12 August 2006]

<sup>4</sup>Visit [www.fcc.gov/cgb/consumerfacts/cipa.html](http://www.fcc.gov/cgb/consumerfacts/cipa.html) for additional information on CIPA.

When this edition of *Guidelines and Resources for Internet Safety in Schools* went to press, a Senate bill, Protecting Children in the 21st Century Act, was pending. This bill would require schools receiving federal E-Rate funds to educate students about Internet safety and block students' access to *social-networking* Web sites and *chat rooms* unless supervised.

All new federal legislation related to Internet safety may be accessed through the Library of Congress's *THOMAS* site at <http://thomas.loc.gov/> or Cornell's U.S. Code Collection: Education at [www4.law.cornell.edu/uscode/html/uscode20/](http://www4.law.cornell.edu/uscode/html/uscode20/).

State legislation may be searched via the Virginia General Assembly's *Legislative Information System* at <http://leg1.state.va.us/061/lis.htm>.



## Issues School Divisions Must Address

As stated in the 2006 legislation, each Virginia school division must add a comprehensive Internet safety component to its acceptable use policy. The division should review its existing acceptable use policy carefully to determine if the Internet safety component will affect other sections. The division then will draft and submit the revised policy to the state Department of Education, which will review the program for compliance.

Although the various Internet safety programs across the state will share some common elements, each division should examine its resources and requirements closely and fashion an appropriate plan that includes the following:

- Integration of Internet safety into the K-12 curriculum and instruction
- Defined roles and responsibilities for the school board; administrators (central office and building); teachers; counselors; instructional technology resource teachers; library media specialists; building resource officers; technology coordinators; students; and community stakeholders, including but not limited to parents, caregivers, public library staff, after-school and off-campus program instructors, and local law enforcement officials
- Safety measures, including any that already exist
- Data and network security plan
- Procedures to address breaches of Internet security and protect students' safety
- Process for annually reviewing, evaluating, and revising the program
- Professional development opportunities for staff across the division
- Outreach programs for community stakeholders

In revising acceptable use policies, divisions will confront three major issues regarding appropriate and effective Internet use—safety, security, and ethics. Since the existing policies already address Internet ethics, the guidelines in this document focus primarily on safety and security topics.

- **The Internet as a valuable tool.** Like any other tool, the Internet can be misused or dangerous in certain circumstances. Students must learn how to use the Internet safely and effectively.

- **Personal safety on the Internet.** Students must understand that people are not always who they say they are. They should never give out personal information without an adult's permission, especially if it conveys where they can be found at a particular time. They should understand that predators are always present on the Internet. Students should recognize the various forms of *cyberbullying* and know what steps to take if confronted with that behavior.
- **Information on the Internet.** Students and their families should discuss how to identify acceptable sites to visit and what to do if an inappropriate site is accessed. Students should be informed about various Web advertising techniques and realize that not all sites provide truthful information.
- **Activities on the Internet.** Likewise, students and their families should discuss acceptable *social networking* and communication methods and the appropriate steps to take when encountering a problem. Students should know the potential dangers of e-mailing, gaming, downloading files, and *peer-to-peer computing* (e.g., *viruses*, legal issues, harassment, sexual predators, *identity theft*).

Each school division should outline options for presenting Internet safety instruction to students. A pilot of the instruction program, coupled with a review of related materials, is recommended prior to divisionwide implementation. The division needs to develop an evaluation component that continually examines the program's effectiveness and recommends revisions.

A frequently overlooked element is school and community support for the acceptable use policy. All stakeholders—division staff and community members—need accurate up-to-date facts. This document is organized by stakeholder group to help divisions define each role clearly.

In addition, all school personnel should keep abreast of constantly changing Internet safety information and communicate regularly on the topic. Some Internet threats, such as bullies and sexual predators, exist in the community as well. As a result, administrators, counselors, and resource officers previously have confronted some of the problems now emerging on the Internet. Division and school personnel also should tap into community resources, such as law enforcement agencies and technology companies that can lend their own expertise.

While devising the revised policy, remember that students may not recognize virtual-life safety issues as readily as real-life safety issues. Virtual-life risks often are invisible, unsolicited, and instant. The division should educate students to recognize potential illegal activities and outline a clear process for reporting problems.

As work commences on the Internet safety component, divisions should refer regularly to the guidelines in this document, the Department of Education's *Acceptable Use Policies*:

*A Handbook* ([www.doe.virginia.gov/VDOE/Technology/AUP/home.shtml](http://www.doe.virginia.gov/VDOE/Technology/AUP/home.shtml)), and existing national Internet safety resources (see Appendix D).

Some divisions already have existing Internet safety programs but should consider expanding them to cover all components recommended in these guidelines. In particular, Internet safety instruction should involve all teachers and be integrated into the curricula.

### *Integrating Internet Safety into Curriculum Content Instruction*

The 2006 legislation requires divisions to integrate the new Internet safety component within the curriculum. School divisions need to design the program specifically to each grade level. Students should learn about Internet safety from kindergarten through high school graduation, acquiring new skills each year while being reminded of previous lessons. All instructors, not just library media specialists or computer-lab teachers, should teach Internet safety and take every opportunity to warn of potential dangers and model safe and appropriate Internet use.

Some Standards of Learning blend naturally with Internet safety lessons. Appendix C lists the Standards of Learning for Computer/Technology that address both Internet safety and ethics issues. The state Department of Education has also published supplemental resources that illustrate how Internet safety lessons can be integrated into core curricular Standards of Learning and which identify ways in which library media specialists can include Internet safety components in their own Linking Libraries lessons. See <http://www.doe.virginia.gov/VDOE/Technology/OET/internet-safety-guidelines.shtml> for links to these resources.

Teachers also can use technology to stress core issues or help students improve essential skills. For instance, when students are creating a project using digital images, a teacher can use this opportunity to demonstrate how easily images can be manipulated and posted to a Web site. As another example, a classroom puppet show could underscore how an unseen person pretends to be someone else—just as some people take on different persona in chat rooms. Students researching online should always try to ascertain the author or host of a Web site and understand that personal and political agendas can influence the information. An interesting student assignment might be to compare how different Web sites present information on the same topic.

In Appendix D, “Student Instruction: Lesson Plans/Curricula” includes examples of Internet safety integrated into curricula; some suggest specific activities for appropriate grade levels. Instructional technology resource teachers can incorporate some of these into professional development or training programs for classroom teachers and library media specialists. Appendix D also includes resources and activities for students, parents, teachers, counselors, library media specialists, resource officers, and administrators. The list is not comprehensive but provides a starting point for locating Internet safety resources.



## What Students Need to Know

*The Internet is a powerful tool that should be used wisely.*

- The Internet allows students access to a vast library of previously unavailable resources.
- The Internet enables students to communicate with people around the world.
- The Internet provides a creative outlet for students skilled in writing, art, music, science, mathematics, and other topics.

### Clicky's Web World: What 2 Do on the Web (NetSmartzKids)

<http://www.netsmartzkids.org/activities/clwebworld/clwhat2do.htm>

### Safe Teens (SafeTeens)

<http://www.safeteens.com/>

**See Appendix D for additional resources.**



*Students need to know that not all Internet information is valid or appropriate.*

- Sexually explicit material or violent images can affect students negatively.
- Sexual predators will try to convince students to trust them.
- Internet information may promote negative attitudes, such as hate or intolerance, and dangerous or illegal activities, such as self-injuring behavior, gambling, and illegal drug use.

*Students should be taught specifically how to maximize the Internet's potential while protecting themselves from potential abuse.*

### Get Your Web License (PBS KIDS)

<http://pbskids.org/license/>

### Tips by Teens for Teens (GetNetWise)

<http://kids.getnetwise.org/safetyguide/teens>

**See Appendix D for additional resources.**



- The critical-thinking skills students learn in the classroom, library, and lab should be applied to Internet resources and Web searching.
- Students need to know what to do and who to ask for help when they encounter a person or site on the Internet that is offensive or threatening to them.
- Students and adults are strongly encouraged to be responsible citizens. Report illegal Internet communications and activities to Internet Service Providers and local law enforcement authorities.

*Internet messages and the people who send them are not always what or who they seem.*

- People in *chat rooms*, *instant message* “buddies,” or those who visit a *blog* may not be who they appear to be. Students should learn to recognize when someone is potentially dangerous.
- Students need to realize when an Internet encounter may be questionable and how to protect themselves when this occurs.
- E-mail can cause *malicious code*-infection problems for a computer or network. Students should not open e-mail or attachments from unknown sources.
- Students need to know which information is safe to share with others online, which should never be shared, and why sharing it could put them at risk.
- Students never should reveal online any information about where they live or attend school.
- Students need to be aware their electronic messages, even those with known friends, can leave *electronic footprints* that can be misused by others.

**iKeepSafe Internet Safety Coalition**

[http://ikeepsafe.org/iksc\\_statemessage/state.php?abbr=VA](http://ikeepsafe.org/iksc_statemessage/state.php?abbr=VA)

**Don't Believe the Type: Surf Safer (Cybertipline)**

<http://tcs.cybertipline.com/surfsafer.htm>

**See Appendix D for additional resources.**



*Predators and cyberbullies anonymously use the Internet to manipulate students. Students must learn how to avoid dangerous situations and get adult help.*

- Sexual predators deceive students by pretending to be students themselves. They sometimes lure young people into a false sense of security or blind trust and try to alienate them from their families. Students need to learn about these types of psychological ploys and how to get immediate adult help.
- Bullies use Internet tools, such as *instant messaging* and the Web, to harass or spread false rumors about students. Students need to know how to seek proper help in these potentially dangerous situations.
- Students need to know that posting personal information and pictures can allow predators to contact and begin *grooming* them for illegal meetings and actions. Personal photos can be easily misused or altered when posted on the Internet.

**Cyberbullies (McGruff)**

<http://www.mcgruff.org/Advice/cyberbullies.php>

**Internet Super Heroes: Cyberbullying (use pull-down menus at bottom) (WiredSafety)**

<http://www.internetsuperheroes.org/cyberbullying/index.html>

**See Appendix D for additional resources.**



*Internet activities, such as playing games and downloading music or video files, can be enjoyable. Students need to know which activities are safe and legal.*

- *Gaming* sites can attract sexual predators and/or *cyberbullies*.
- Some games may contain pornographic and/or violent images. Students need to talk with parents about what is acceptable.
- Students need to know how to detect whether a specific file download is legal and/or free of *malicious code*.

**10 Tips for Dealing with Game Cyberbullies and Griefers (Microsoft)**

<http://www.microsoft.com/protect/family/activities/griefers.msp>

**The 411: File Sharing (StaySafe)**

<http://www.staysafe.org/teens/411/filessharing.html>

**See Appendix D for additional resources.**





## What Parents, Grandparents, and Caregivers Need to Know

*The Internet is a valuable learning, communication, and entertainment provider. A child's Internet use should be based on age and the family's needs and values.*

- The Internet can help with research and homework.
- The Internet can facilitate easy communications with family members and friends.
- Although the Internet can be educational and entertaining, children should spend time offline.
- Appropriate Internet activities for children should be age related. Teenage activities may not be appropriate for a young child.

**Online Safety Guide (click on age-level tips on left side of screen) (GetNetWise)**

<http://kids.getnetwise.org/safetyguide/>

**Parenting Online (WiredKids)**

<http://wiredkids.org/resources/documents/pdf/parentingonline.pdf>

**See Appendix D for additional resources.**



*Parents must understand potential Internet dangers and prepare their children, just as they prepare them for going to the playground or crossing the street.*

**Internet Safety: Information for Parents (WiredSafety)**

<http://www.wiredsafety.org/parent.html>

**Online Predators: Help Minimize the Risk (Microsoft)**

<http://www.microsoft.com/protect/family/guidelines/predators.msp>

**See Appendix D for additional resources.**



- The Internet contains inappropriate information for children, such as pornography, hate literature, aggressive advertising, and violent images.
- Internet communication often is anonymous, especially in *chat rooms* or *blogs*. A sexual predator may pose as a friend to lure a child away from his or her family's protection. *Cyberbullies* may target a child for harassment.

- Using e-mail or downloading files can lead to *viruses* or hidden *spyware*, which endanger a family's privacy and computer.
- Information provided over the Internet—by children and adults—can be used for *identity theft*.

***Parents can provide the best protection for their children and help reinforce the principles learned in the classroom. Families should reach agreements about acceptable Internet activity and content.***

- Parents should read about and know how to respond to Internet risks. They can stay informed by signing up for a family Internet safety newsletter (see “Newsletters” in Appendix D) and working directly with their school divisions.
- Parents should talk with their children about safe and appropriate Web sites and activities.
- Children should be encouraged to report anything they feel uneasy about. If parents overreact, children will be less likely to confide in them the next time.
- The family should create rules about what children can and cannot do while online. Posting the agreements near the computer will ensure children see them often.

**The Children’s Partnership: The Parents’ Guide to the Information SuperHighway**

[http://www.childrenspartnership.org/AM/Template.cfm?Section=Speeches\\_and\\_Presentations&CONTENTID=4687&TEMPLATE=/CM/HTMLDisplay.cfm](http://www.childrenspartnership.org/AM/Template.cfm?Section=Speeches_and_Presentations&CONTENTID=4687&TEMPLATE=/CM/HTMLDisplay.cfm)

**staysafe.org for Parents**

<http://www.msn.staysafeonline.com/parents/default.html>

**See Appendix D for additional resources.**



***Monitoring is crucial. Parents should know where their children go online, how long they stay there, and the warning signs that something is wrong.***

- Parents should place computers in family areas as opposed to bedrooms; however, they need to realize that *instant messaging* devices, cell phones, and *wireless computers* may allow children to get online anywhere.
- When young children first begin going online, parents should work closely with them and talk about Internet safety at an early age.
- Parents should *bookmark* suitable sites and check back regularly to ensure that the content of those sites has not changed and that harmful sites have not been bookmarked.
- *Filters* are helpful but not fail proof. Parents need to know about *circumventor sites*, which allow users to get around *filtering* software controls.
- Parents should seek training to learn different methods of *monitoring* their children’s Internet use. They continually need to employ up-to-date techniques and software to track where their children go online.
- Parents should be aware that some sites have age restrictions that children may ignore or not realize.

- Parents should follow where their children go on the Internet just as they would watch them in a large public area. They need to check regularly the *history* and *bookmarks* or *favorites* on all computers in the house.
- Parents should recognize the warning signs of when a child might be in trouble, doing something they should not be doing, or spending too much time on the Internet. They should know how to report a problem to their Internet Service Provider and local law enforcement officials.
- Some Internet activities are not only dangerous but illegal. Parents should be aware of relevant laws.

**Filter Review (National Coalition for the Protection of Children and Families)**

<http://www.filterreview.com/index.htm>

**Cybertipline (National Center for Missing and Exploited Children)**

<http://www.cybertipline.com/>

**See Appendix D for additional resources.**





# What Teachers, Instructional Technology Resource Teachers, Library Media Specialists, Counselors, and Resource Officers Need to Know

*Classroom Internet use can be exciting, rewarding, and challenging. Students' Internet use should be tailored to their ages.*

- Teachers should create age-appropriate activities for students.
- Students' varying developmental stages and Internet skills will produce different issues and problems for each age group.
- Educators should maintain open communication with parents about students' academic Internet use—in guided classroom settings and independently.

## Child Safety Tips: Age-Based Guidelines for Kids' Internet Use (Microsoft)

<http://www.microsoft.com/protect/family/age/stages.aspx>

## Online Risks (NetSmartz)

<http://www.netsmartz.org/safety/risks.htm>

**See Appendix D for additional resources.**



## *Monitoring is crucial.*

- *Filters* are not fail proof. Teachers and librarians must watch where students go on the Internet—just as they would keep an eye on them during a field trip. Computer labs may be configured to assist with this supervision.
- Students should not be allowed to wander aimlessly on the Internet. Teachers must provide an academic purpose before allowing students to go online.
- Teachers need to acquaint themselves with new tools that allow students to visit protected sites. As much as possible, they should go into *history* and examine the pages students have viewed.
- Classroom and library rules must comply with the division's acceptable use policy regarding the steps students should take after accidentally accessing an inappropriate site.
- Technical staff need to utilize the division's network tracking controls and study the generated reports, which may identify patterns of inappropriate use.

## Parents & Educators (McGruff)

<http://www.mcgruff.org>

## How To (staysafe.org)

[http://www.msn.staysafeonline.com/toolbox/how\\_to/index.html](http://www.msn.staysafeonline.com/toolbox/how_to/index.html)

**See Appendix D for additional resources.**



- Teachers need to keep up-to-date on Internet safety issues and provide accurate, timely information to students.

*Student technological interactions in the virtual world can be negative and spill over into the real world.*

- Educators need to learn about *cyberbullying*, recognize the signs of a bullied student, and know what to do about it.
- Students must be taught which types of personal information are safe to share with others.
- Online and wireless communications—even with known friends or peers—can compromise students’ privacy as technology-savvy predators may eavesdrop.
- Students must understand that people are not always who they claim to be and that Internet information is not always accurate or appropriate.

**Cyberbullying (Cyberbullying.org)**

<http://www.cyberbullying.org/>

**Social Networking and Schools (Childnet International)**

<http://www.childnet-int.org/blogsafety/teachers.html>

**See Appendix D for additional resources.**



*Exchanging information with others is a great way to use the Internet but also possesses inherent dangers.*

**Risks by Technology: Email (GetNetWise)**

<http://kids.getnetwise.org/safetyguide/technology/email>

**Young People, Music & the Internet (P2P) (Childnet International)**

<http://www.childnet-int.org/music/parents.html>

**See Appendix D for additional resources.**



- Educators must know and enforce school policies on exchanging or downloading files.
- School staff should be alerted continually about potential e-mail dangers and learn how to recognize the problem signs.
- Online journals and *blogs*, even when password-protected, may reveal more personal information than a student intends. Technology-savvy predators can circumvent many safeguards offered by journal and *blogging* sites.
- Educators should check the age appropriateness of any *social-networking* sites that students visit.

## *Students need to hear the rules often.*

- Teachers should establish and post rules for safe Internet use near computers in classrooms, libraries, and labs. Students should be reminded regularly that the rules are intended to ensure their safety.
- Teachers should go over the rules with students periodically. As a result, the students—even when excited or upset—will be more likely to remember the rules.
- Students and their parents should know the consequences of disobeying the rules. Educators must keep the lines of communication open with students and parents.
- Schools must be consistent and fair in enforcing classroom rules and the division's acceptable use policy.

### **Kids' Rules for Online Safety (SafeKids.com)**

<http://www.safekids.com/kidsrules.htm>

### **Common Sense Rules Can Protect Kids on the Net (SafeKids)**

<http://www.safekids.com/commonsense.htm>

**See Appendix D for additional  
resources.**





## What School Administrators Need to Know

School administrators should play key roles in developing and implementing a division policy that protects children on the Internet. They ultimately must enforce the division's acceptable use policy and Technology Standards for Instructional Personnel (TSIP) and understand the information needs of all stakeholders: teachers, instructional technology resource teachers, technology personnel, library media specialists, counselors, principals, resource officers, parents, local law enforcement agencies, and civic organizations.

*Administrators must oversee all aspects of the Internet safety program.*

- Review annually the division's technology infrastructure with appropriate technology staff, making improvements as needed.
- Monitor the quality and effectiveness of Internet safety information presented to the respective stakeholder groups.
- Incorporate Internet safety into the division's professional development plans and community outreach programs.
- Schedule continuing professional development to keep educators aware of the most recent Internet safety developments.

*The Internet is invaluable, educationally and administratively; however, as with all tools, it can be misused and dangerous. In addition, the Internet constantly changes.*

- Administrators should understand the Internet's educational advantages and how it is used throughout the division.
- Administrators must understand the potential risks of using the (1) Internet for instruction and (2) technology networks for data collection, storage, and communication.
- Administrators should stay up-to-date with new developments in capabilities, vulnerabilities, and legal issues related to the Internet and school responsibilities.
- Schools should appoint a staff member—a security officer or other appropriate person—to make sure this policy is implemented.

*As with any system, the division must have clear and effective policies and procedures in place to protect students and help prevent misuse of the system. In addition, policies and procedures must be in place for crisis management.*

- A systematic review of policies and procedures needs to be carried out at least yearly.
- Since risks cannot be completely eliminated, the division should be prepared to handle a crisis.

- *Filters* are helpful but not fail proof. As students become more experienced, they may use *circumventor sites* to get around *filtering* software controls.
- Funding for security and safety technology should be anticipated and planned.

*Communication among all stakeholders is imperative for safety and security policies to be effective. Although a school's legal responsibility does not extend to home Internet use, school leaders can help prevent tragic situations by ensuring parents and students are well-informed.*

- Administrators should inform parents regularly about new Internet safety information.
- Students and parents must know the policies and the consequences associated with violations.
- Professional development on Internet safety must be a high priority.
- Funding needs to be budgeted regularly for better communication and training, which must be evaluated for its effectiveness.
- The acceptable use policy's Internet safety component should clearly emphasize that protecting children is a high priority.

#### **Cyber Security for the Digital District**

<http://securedistrict.cosn.org/index.html>

#### **Internet Safety Policies and CIPA: An E-Rate Primer for Schools and Libraries**

[http://www.e-ratecentral.com/CIPA/cipa\\_policy\\_primer.pdf](http://www.e-ratecentral.com/CIPA/cipa_policy_primer.pdf)

**See Appendix D for additional resources.**





## What School Boards Need to Know

Each school board must review and approve its division's revised acceptable use policy and implementation plan as presented by the superintendent. The board must ensure the policy complies with current federal, state, and local laws relating to Internet safety.

*The Internet is invaluable, educationally and administratively; however, as with all tools, it can be misused and dangerous. In addition, the Internet constantly changes.*

- The board should understand the Internet's educational advantages and how it is used in the division.
- The board must understand the potential risks of using the (1) Internet for instruction and (2) technology networks for data collection, storage, and communication.
- Board members should stay up-to-date with new developments in capabilities, vulnerabilities, and legal issues related to the Internet and school responsibilities.

*As with any system, the division must have clear and effective policies and procedures to protect students and prevent misuse. Policies and procedures also must be in place for crisis management.*

- A systematic review of policies and procedures needs to be carried out at least yearly.
- Since risks cannot be completely eliminated, the division should be prepared to handle a crisis.
- Funding for security and safety technology should be anticipated and planned.

*Communication among all stakeholders is imperative for safety and security policies to be effective. Although school legal responsibility may not extend to home Internet use, school staff can help prevent tragic situations by ensuring parents and students are well-informed.*

- Providing information to parents should be a priority.
- Students and parents must know the policies and the consequences associated with violations.
- Professional development for all educators on Internet safety should be a high priority.
- Funding needs to be budgeted regularly for better communication and training, which must be evaluated for its effectiveness.

**National School Boards Association Technology Page**

<http://www.nsba.org/site/page.asp?TRACKID=&CID=397&DID=8638>

See also:

<http://www.nsba.org/site/page.asp?TRACKID=&CID=394&DID=8635>.

**Education Law Organization**

<http://www.educationlaw.org/>

**Virginia Department of Criminal Justice Services: Virginia Center for School Safety**

<http://www.dcjs.virginia.gov/vcss/>

**Family Internet Safety (Attorney General of Virginia)**

[http://www.oag.state.va.us/KEY\\_ISSUES/FAMILY\\_INTERNET/index.html](http://www.oag.state.va.us/KEY_ISSUES/FAMILY_INTERNET/index.html)

**See Appendix D for additional resources.**





# Appendix A

## CHAPTER 52

*An Act to amend and reenact § 22.1-70.2 of the Code of Virginia, relating to Internet safety instruction in schools.*

[H 58]

Approved March 7, 2006

Be it enacted by the General Assembly of Virginia:

1. That § 22.1-70.2 of the Code of Virginia is amended and reenacted as follows:

§ 22.1-70.2. Acceptable Internet use policies for public and private schools.

A. Every two years, each division superintendent shall file with the Superintendent of Public Instruction an acceptable use policy, approved by the local school board, for the international network of computer systems commonly known as the Internet. At a minimum, the policy shall contain provisions that (i) are designed to prohibit use by division employees and students of the division's computer equipment and communications services for sending, receiving, viewing, or downloading illegal material via the Internet; (ii) seek to prevent access by students to material that the school division deems to be harmful to juveniles as defined in § 18.2-390; (iii) select a technology for the division's computers having Internet access to filter or block Internet access through such computers to child pornography as set out in § 18.2-374.1:1 and obscenity as defined in § 18.2-372; (iv) establish appropriate measures to be taken against persons who violate the policy; and (v) include a component on Internet safety for students that is integrated in a division's instructional program. The policy may include such other terms, conditions, and requirements as deemed appropriate, such as requiring written parental authorization for Internet use by juveniles or differentiating acceptable uses among elementary, middle, and high school students.

B. The superintendent shall take such steps as he deems appropriate to implement and enforce the division's policy.

C. On or before December 1, 2000, and biennially thereafter, the Superintendent of Public Instruction shall submit a report to the Chairmen of the House Committee on Education, the House Committee on Science and Technology, and the Senate Committee on Education and Health which summarizes the acceptable use policies filed with the Superintendent pursuant to this section and the status thereof.

D. In addition to the foregoing requirements regarding public school Internet use policies, the principal or other chief administrator of any private school that satisfies the compulsory school attendance law pursuant to § 22.1-254 and accepts federal funds for Internet access shall select a technology for its computers having Internet access to filter or block Internet access through such computers to child pornography as set out in § 18.2-374.1:1 and obscenity as defined in § 18.2-372.

*E. The Superintendent of Public Instruction shall issue guidelines to school divisions regarding instructional programs related to Internet safety.*

2. That, within 45 days of the enactment of this act, the Superintendent of Public Instruction shall issue a superintendent's memorandum advising school divisions of the provisions in this act and encourage cooperation with local law-enforcement agencies in its implementation.



## Appendix B

COMMONWEALTH OF VIRGINIA  
DEPARTMENT OF EDUCATION  
P.O. BOX 2120  
RICHMOND, VIRGINIA 23218-2120

SUPTS. MEMO NO.15  
April 21, 2006

### ADMINISTRATIVE

TO: Division Superintendents

FROM: Patricia I. Wright  
Acting Superintendent of Public Instruction

SUBJECT: Internet Safety Instruction in Schools

Legislation approved by the 2006 General Assembly and signed by Governor Kaine adds a requirement to the acceptable Internet use policies developed by the division superintendents that such policies include a component on Internet safety for students. This legislation can be found at the following address:

<http://leg1.state.va.us/cgi-bin/legp504.exe?061+ful+CHAP0052+pdf>

The Internet safety component must be integrated within a division's instructional program. This legislation also requires the Superintendent of Public Instruction to issue guidelines to school divisions regarding instructional programs related to Internet safety.

The purpose of this memorandum is to communicate to you the provisions of this important piece of legislation and to encourage you to share with this department any well-established resources used by your division to ensure the safe use of the Internet by students in your schools. Since the department is currently in the early stages of drafting guidelines related to this legislation, this is an opportune time to gather resource information from school divisions for inclusion in the guidelines. It is the department's intent to draft guidelines over the summer for release prior to the beginning of the 2006-2007 school year.

Should you have information that you would like to have considered during guideline development, please provide the following to the department:

- ✓ A brief description of the Internet safety program currently used within the division and the length of time that the program has been in place.
- ✓ All applicable public Web site addresses where such information is available.

Please send all information no later than May 26, 2006, to Charlie Makela, School Library Media Programs & Research Services specialist, at [Charlie.Makela@doe.virginia.gov](mailto:Charlie.Makela@doe.virginia.gov). You may also contact Ms. Makela directly at (804) 786-9412, should you have any questions.

PIW/ADW/fmc



## Appendix C

### *Internet Safety and the Virginia Standards of Learning for Computer/Technology for Grades K-12*

#### **Social and Ethical Issues**

- C/T K-2.3      The student will practice responsible use of technology systems, information, and software.
- Know the school's rules for using computers.
  - Understand the importance of protecting personal information or passwords.
  - Understand the basic principles of the ownership of ideas.
- C/T K-2.4      The student will use technology responsibly.
- Demonstrate respect for the rights of others while using computers.
  - Understand the responsible use of equipment and resources.
- C/T 3-5.3      The student will demonstrate knowledge of ethical, cultural, and societal issues related to technology.
- Identify how technology has changed society in areas such as communications, transportation, and the economy.
  - Discuss ethical behaviors when using information and technology.
- C/T 3-5.4      The student will practice responsible use of technology systems, information, and software.
- Understand the need for the school division's acceptable use policy.
  - Discuss the rationale of fair use and copyright regulations.
  - Follow rules for personal safety when using the Internet.
- C/T 3-5.5      The student will demonstrate knowledge of technologies that support collaboration, personal pursuits, and productivity.
- Work collaboratively when using technology.
  - Practice and communicate respect for people, equipment, and resources.
  - Understand how technology expands opportunities for learning.
- C/T 6-8.3      The student will demonstrate knowledge of ethical, cultural, and societal issues related to technology.
- Demonstrate knowledge of current changes in information technologies.
  - Explain the need for laws and policies to govern technology.
  - Explore career opportunities in technology-related careers.
- C/T 6-8.4      The student will practice responsible use of technology systems, information, and software.
- Demonstrate the correct use of fair use and copyright regulations.
  - Demonstrate compliance with the school division's Acceptable Use Policy and other legal guidelines.
- C/T 6-8.5      The student will demonstrate knowledge of technologies that support collaboration, personal pursuits, and productivity.
- Work collaboratively and/or independently when using technology.
  - Practice preventative maintenance of equipment, resources, and facilities.

- Explore the potential of the Internet as a means of personal learning and the respectful exchange of ideas and products.

- C/T 9-12.3      The student will demonstrate knowledge of ethical, cultural, and societal issues related to technology.
- Assess the potential of information and technology to address personal and workplace needs.
  - Demonstrate knowledge of electronic crimes such as viruses, pirating, and computer hacking.
  - Explore and participate in online communities, and online learning opportunities.
  - Identify the role that technology will play in future career opportunities.
- C/T 9-12.4      The student will practice responsible use of technology systems, information, and software.
- Adhere to fair use and copyright guidelines.
  - Adhere to the school division's Acceptable Use Policy as well as other state and federal laws.
  - Model respect for intellectual property.
- C/T 9-12.5      The student will demonstrate knowledge of technologies that support collaboration, personal pursuits, and productivity.
- Respectfully collaborate with peers, experts, and others to contribute to an electronic community of learning.
  - Model responsible use and respect for equipment, resources, and facilities.



## Appendix D

### Web-Based Resources on Internet Safety

This appendix lists Web sites related to Internet safety. All Web sites were accurate and online as of September 12, 2007. An online version of this appendix which is updated on a regular basis may be found at <http://www.doe.virginia.gov/VDOE/Technology/OET/internet-safety-guidelines.shtml>.

#### Age-Appropriate Guidelines for Internet Use

*Age-Based Guidelines for Kids' Internet Use* by Microsoft

<http://www.microsoft.com/athome/security/children/parentsguide.msp>

- Guide to how children of different ages use the Internet

*Be Web Aware* by Media Awareness Network (see Safety Tips by Age on left side of screen)

<http://www.bewebaware.ca/english/default.aspx>

- Safety tips by age (left-side menu)

*GetNetWise: Online Safety Guide* by Internet Education Foundation

<http://kids.getnetwise.org/safetyguide/>

- A parent's perspective and information about online privacy

#### Copyright (see Ethics)

#### Cyberbullying

*Be Web Aware: Challenging Cyber Bullying* by Media Awareness Network

<http://www.bewebaware.ca/english/CyberBullying.aspx>

- Legal overview, role of Internet service providers, and taking action

*Cyberbullies* by National Crime Prevention Council

<http://www.mcgruff.org/Advice/cyberbullies.php>

- Tips for avoiding and handling *cyberbullies*

Cyberbully home page by Cyberbully.org (Nancy Willard)

<http://www.cyberbully.org/>

- Very helpful information with several downloadable handouts

*Cyberbullying: Research* by Cyberbully.us

<http://www.cyberbullying.us/research.php>

- Research and other helpful information

Cyberbullying handouts [untitled] by Bullying.org

[http://www.cyberbullying.org/pdf/Cyberbullying\\_Information.pdf](http://www.cyberbullying.org/pdf/Cyberbullying_Information.pdf)

- Details about *cyberbullying* (Canadian)

*OnGuard Online—US CERT Tip: Dealing with Cyberbullies* by United States Computer Emergency Readiness Team

<http://www.onguardonline.gov/certtips/st06-005.html>

- Recognition of and protection from *cyberbullies*

*Real-Life Stories* by NetSmartz

<http://www.netsmartz.org/resources/reallife.htm>

- Stories and videos about the impact of *cyberbullying* on kids

*STOP cyberbullying* by WiredKids

<http://www.stopcyberbullying.org/index2.html>

- Legal overview, prevention, and reporting

*Stoptextbully.com* by NCH

<http://www.stoptextbully.com/>

- Downloadable posters

## Definitions

*BeWebAware: Internet 101* by Media Awareness Network

<http://www.bewebaware.ca/english/internet101.aspx>

- Short glossary of several Internet terms

*Glossary* by Symantec

<http://securityresponse.symantec.com/avcenter/refa.html>

- Extensive glossary of computer terms

*Internet Definitions* by Netsmartz

<http://www.netsmartz.org/safety/definitions.htm>

- Extensive online glossary

*The Librarian's Guide to Great Web Sites for Kids* by American Library Association

<http://www.ala.org/parentspage/greatsites/guide.html>

- Definitions of new technologies (end of paper)

*OnGuard Online: Glossary* by Federal Trade Commission

<http://onguardonline.gov/glossary.html>

- Standard glossary of computer terms

## E-mail

*BeWebAware: Spam* by Media Awareness Network

<http://www.bewebaware.ca/english/spam.aspx>

- Tips for parents regarding *spam*

*GetNetWise: Risks by Technology: Email* by Internet Education Foundation

<http://kids.getnetwise.org/safetyguide/technology/email>

- Basic overview of *spam* and junk mail

*Help Keep Spam Out of Your Inbox* by Microsoft

<http://www.microsoft.com/athome/security/email/fightspam.msp>

- Tips and *filters* for blocking junk mail

*OnGuard Online: Spam Scams* by Federal Trade Commission

<http://onguardonline.gov/spam.html>

- List of popular scams and recommendations for avoiding problems

*Sorted: Keep Your Information Secure Online* by Childnet International

<http://www.childnet-int.org/sorted/>

- Maintaining student safety and privacy

## Ethics

*Acceptable Use Policies: A Handbook* by the Virginia Department of Education

<http://www.doe.virginia.gov/VDOE/Technology/AUP/home.shtml>

- Virginia's handbook for creating acceptable use policies with links to resources on cyberethics and *filtering*

*Cyberethics* by U.S. Department of Justice, Computer Crime & Intellectual Property Section

<http://www.cybercrime.gov/cyberethics.htm>

- Links to sites about *cybercrime*

*RespectCopyrights.org* by Motion Picture Association of America

<http://www.respectcopyrights.org/content.html>

- Issues involved with illegal downloads

## Filtering

*BeWebAware: Get the Most out of the Internet: Technological Tools* by Media Awareness Network

[http://www.media-awareness.ca/english/teachers/wa\\_teachers/safe\\_passage\\_teachers/getmost\\_techtools.cfm](http://www.media-awareness.ca/english/teachers/wa_teachers/safe_passage_teachers/getmost_techtools.cfm)

- Checklist for evaluating content-management products and related issues

*Filtering and Blocking* by WiredKids

<http://www.wiredkids.org/safesites/filtering.html>

- Information about *filtering*, blocking, and outgoing software

*FilterReview.com* by National Coalition for the Protection of Children and Families

<http://www.filterreview.com/index.htm>

- Background for selecting the most appropriate *filters*

“Why Filters Won’t Protect Children or Adults” by Nancy Kranich, *Library Administration and Management* 18(1): 14-18 (published by American Library Association)

<http://www.ala.org/ala/oif/ifissues/issuesrelatedlinks/whyfilterswontprotect.htm>

- Educating about Internet safety as opposed to using *filters*

*The X Lab: Internet Safety for Children* by The X Lab

<http://www.thexlab.com/faqs/internetsafetychild.html>

- Listing of *filtering* software for Macs

## Hate Sites

*BeWebAware: Violent and Hateful Content* by Media Awareness Network

<http://www.bewebaware.ca/english/violent.aspx>

- Information about violent content, online hate, and what parents should do

*Hate on the Internet: A Response Guide for Educators and Families* by Partners Against Hate

[http://www.partnersagainsthate.org/publications/hoi\\_full.pdf](http://www.partnersagainsthate.org/publications/hoi_full.pdf)

- Advice and tools for helping students manage exposure to hate sites

*Protecting Children and Teens from Online Hate* by Media Awareness Network

[http://www.media-awareness.ca/english/issues/online\\_hate/protect\\_child\\_hate.cfm](http://www.media-awareness.ca/english/issues/online_hate/protect_child_hate.cfm)

- An overview of hate sites, laws, and how to help students deconstruct them

WHOIS Search by Network Solutions

<http://www.networksolutions.com/whois/index.jsp>

- Search engine to determine ownership of domain names

## How the Internet Works

*How Does the Internet Work?* By U&I Learning (commercial site—no advertising)

<http://hwi.uni.be/archief/en/index.htm>

- Animated modules that explain how the Internet works

*How Internet Infrastructure Works* by Jeff Tyson for HowStuffWorks

<http://computer.howstuffworks.com/internet-infrastructure.htm>

- An illustrated article that explains the underlying structure of the Internet

*HQ: Introduction* by For Kids By Kids Online (Cyberspace Research Unit-UK)

<http://www.fkbko.co.uk/EN.php?lang=EN&&subject=1&&id=0&&level=0>

- An illustrated explanation of how the Internet works in the context of Internet Safety for kids

*The Internet Tutorial* by Dynamic Web Solutions (commercial site—no advertising)

<http://www.dynamicwebs.com.au/tutorials/history.htm>

- Tutorials that explain the workings of the Internet

## Identity Theft

*Fighting Back against Identity Theft* by Federal Trade Commission

<http://www.ftc.gov/bcp/edu/microsites/idtheft/>

- Resources about *identity theft*, including a printable brochure and PowerPoint slides

*Keep Your Identity To Yourself* by National Crime Prevention Council

[http://www.ncpc.org/media/Identity\\_Theft.php](http://www.ncpc.org/media/Identity_Theft.php)

- Free download of *Preventing Identity Theft: A Guide for Consumers*

*OnGuard Online: ID Theft* by Federal Trade Commission

<http://onguardonline.gov/idtheft.html>

- Steps to take in case of *identity theft*

*Recognize Phishing Scams and Fraudulent E-mails* by Microsoft

<http://www.microsoft.com/athome/security/email/phishingemail.mspx>

- Basic overview of *phishing* scams

## Instant Messaging

*10 Tips for Safer Instant Messaging* by Microsoft

<http://www.microsoft.com/athome/security/online/imsafety.mspx>

- Suggestions for using *instant messaging*

## International, National, and State Organizations

ChildNet International home page

<http://www.childnet-int.org>

Cyberbullying.org home page

<http://www.cyberbullying.org/>

*Cyberethics, Cybersafety, Cybersecurity (C3) Institute* by University of Maryland, College of Education  
<http://www.edtechoutreach.umd.edu/C3Institute/c3resources.html>

*Family Internet Safety* by Attorney General of Virginia  
[http://www.oag.state.va.us/KEY\\_ISSUES/FAMILY\\_INTERNET/index.html](http://www.oag.state.va.us/KEY_ISSUES/FAMILY_INTERNET/index.html)

GetNetWise home page by Internet Education Foundation  
<http://www.getnetwise.com/>

*Internet Safety* by Polly Klaas Foundation  
<http://www.pollyklaas.org/internet-safety/index.html>

i-SAFE home page by Internet Safety Foundation  
<http://www.isafe.org/>

*Kidz Privacy* by Federal Trade Commission  
<http://www.ftc.gov/bcp/online/edcams/kidzprivacy/index.html>

National Center for Missing & Exploited Kids home page  
<http://www.missingkids.com/>

*NetSmartz Workshop* by National Center for Missing & Exploited Kids  
<http://www.netsmartz.org/>  
<http://www.netsmartz.org/espanol/> (Spanish)

OnGuard Online home page by Federal Trade Commission  
<http://onguardonline.gov/index.html>

*OnGuard Online: U.S. Computer Emergency Readiness Team* by Federal Trade Commission  
<http://www.onguardonline.gov/certtips/index.html>

Operation Blue Ridge Thunder home page by Bedford County Sheriff's Office  
<http://www.blueridgethunder.com/DefaultHome.asp>

ProtectKids.com home page by Enough Is Enough  
<http://www.protectkids.com/>

SafeKids.com home page  
<http://www.safekids.com/>

Safe Surfin' Foundation home page  
<http://www.safesurfincentral.org/>

Staysafe.org home page  
<http://www.msn.staysafeonline.com/>

Virginia Center for School Safety home page by Virginia Department of Criminal Justice Services  
<http://www.dcjs.virginia.gov/vcss/?menuLevel=5>

Web Wise Kids home page by Web Wise Kids  
<http://www.webwisekids.org/>

WiredSafety.org home page by WiredKids (includes *Teenangels*, *WiredSafety*, and *WiredKids*)  
<http://www.wiredsafety.org/>

## Internet Benefits and Risks

*Cybercrime* by National Association of Attorneys General

- [http://naag.org/publications\\_cybercrime.php](http://naag.org/publications_cybercrime.php)
- Online articles about different aspects of *cybercrime*

*GetNetWise: What are the Risks for Children Online?* by Internet Education Foundation

- <http://kids.getnetwise.org/safetyguide/danger/>
- Overview of various Internet risks

*Parenting Online* by WiredKids

- <http://wiredkids.org/parents/parentingonline/index.html>  
<http://wiredkids.org/resources/documents/pdf/parentingonline.pdf> (printable version)  
<http://www.wiredkids.org/parents/parentingonline/parentingonline-ES-v1.pdf> (Spanish version)
- Internet positives and negatives, plus tips for avoiding problems

*The Positives and Perils of the Internet: Working Together to Make Your Family's Online Experience Safe and Fun* by Donna Rice Hughes for ProtectKids.com

- [http://www.protectkids.com/parentsafety/positive\\_peril.htm](http://www.protectkids.com/parentsafety/positive_peril.htm)
- Safety tips for parents and children

*What Are The Risks* by SafeKids.Com

- <http://www.safekids.com/risks.htm>
- Brief overview of potential risks

## Legal: National

*Class Action: Virginia Students and the Law* by Attorney General of Virginia

- [http://www.oag.state.va.us/KEY\\_ISSUES/CLASS\\_ACTION/](http://www.oag.state.va.us/KEY_ISSUES/CLASS_ACTION/)
- Information about computer crimes (material implemented generally by school resource officers)

Education Law Association home page

- <http://www.educationlaw.org/>
- Developed by educational and legal scholars

*Internet Safety Policies and CIPA: An E-Rate Primer for Schools and Libraries* by E-Rate Central

- [http://www.e-ratecentral.com/CIPA/cipa\\_policy\\_primer.pdf](http://www.e-ratecentral.com/CIPA/cipa_policy_primer.pdf)
- Requirements for federal funding related to the Children's Internet Protection Act (CIPA) and
  - Neighborhood Children's Internet Protection Act (NCIPA)

*School Law in Review 2006* by National School Boards Association

- [https://secure.nsba.org/pubs/item\\_info.cfm?ID=727](https://secure.nsba.org/pubs/item_info.cfm?ID=727)
- CD-ROM, available for purchase, including most aspects of education law

*School Law: Technology* by National School Boards Association

- <http://www.nsba.org/site/page.asp?TRACKID=&CID=397&DID=8638>
- Legal technology information, including resources, news, and recent cases

*SPAM/Technology Crimes: Computer Crime Unit* by Attorney General of Virginia

- <http://www.oag.state.va.us/CONSUMER/SPAM/index.html>
- Overview of *cybercrimes* in the Commonwealth of Virginia

THOMAS by Library of Congress

<http://thomas.loc.gov/>

- Web site of Congress, including searchable database of *cybercrime* laws

U.S. Code Collection by Cornell Law School

<http://www4.law.cornell.edu/uscode/html/uscode20/>

- Past and current U.S. Code chapters related to education, including *cybercrime* issues

Virginia Center for School Safety home page by Virginia Department of Criminal Justice Services

<http://www.dcjs.virginia.gov/vcss/>

- Virginia legislative mandates for school safety

## Legal: Virginia Laws

*Computer fraud*

<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-152.3> § 18.2-152.3

*Computer invasion of privacy*

<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-152.5> § 18.2-152.5

*Computer trespass (hacking/cracking)*

<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-152.4> § 18.2-152.4

*Enhanced penalties for using a computer in certain violations (advertising/producing obscene materials)*

<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-376.1> § 18.2-376.1

*Harassment by computer (cyberbullying)*

<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-152.7C1> § 18.2-152.7:1

*Identity theft*

<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-186.3> § 18.2-186.3

*Personal trespass by computer*

<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-152.7> § 18.2-152.7

*Possession, reproduction, distribution, and facilitation of child pornography*

<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-374.1C1> § 18.2-374.1:1

*Production, publication, sale, financing, etc., of child pornography, presumption as to age*

<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-374.1> § 18.2-374.1

*Property capable of embezzlement (by computer)*

<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-152.8> § 18.2-152.8

*Theft of computer services (WiFi surfing)*

<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-152.6> § 18.2-152.6

*Transmission of unsolicited bulk electronic mail (spam)*

<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-152.3C1> § 18.2-152.3:1

*Use of communications systems to facilitate certain offenses involving children (solicitation)*

<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-374.3> § 18.2-374.3

*Using a computer to gather identifying information (phishing/pharming)*  
<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-152.5C1> § 18.2-152.5:1

## Newsletters, Blogs and Podcasts

*GetNetWise-News* by GetNetWise  
<http://www.getnetwise.com/news/>

*Internet Safety—For Our Children’s Sake* by Jace Shoemaker-Galloway  
<http://internetsafetyadvisor.squarespace.com/journal/>  
• Internet safety *blog* maintained by a Midwestern school leader

*i-SAFE Times, i-EDUCATOR Times, and i-PARENT Times* by i-SAFE  
[http://www.isafe.org/channels/sub.php?ch=op&sub\\_id=4](http://www.isafe.org/channels/sub.php?ch=op&sub_id=4)

*Microsoft Security for Home Computer Users Newsletter* by Microsoft  
<http://www.microsoft.com/athome/security/secnews/default.msp>

*Net Family News*  
<http://netfamilynews.org/letterindex4.html>

*Netsmartz Bulletin* by National Center for Missing & Exploited Children and Boys & Girls Clubs of America  
<http://www.netsmartz.org/feedback/bulletin.htm>

*OnGuard Online: US-CERT Alerts* by Federal Trade Commission  
<http://onguardonline.gov/certalerts.html>

SafeKids.com home page  
<http://safekids.com/>  
• “Timely articles” link features up-to-date information

## Online Games

*Kids & Gaming: Tips for Parents to Helps Kids Play It Safe* by Microsoft  
<http://www.microsoft.com/athome/security/children/gamingonline.msp>  
• Suggestions for keeping children’s *gaming* experiences safe and age appropriate

*Online Gaming Safety* by Wiredsafety.org  
[http://www.wiredsafety.org/safety/chat\\_safety/online\\_gaming\\_safety/index.html](http://www.wiredsafety.org/safety/chat_safety/online_gaming_safety/index.html)  
• An overview of safety related to online *gaming* and a list of safe *gaming* sites

*10 Tips for Dealing with Game Cyberbullies and Grievers* by Microsoft  
<http://www.microsoft.com/athome/security/children/grievers.msp>  
• Suggestions for handling *grievers*, who cause trouble for other online game players

## Parent/Child Sample Agreements

*Family Contract for Online Safety* by SafeKids.com  
<http://www.safekids.com/contract.htm>  
• Kid’s Pledge and Parent’s Pledge

*Kids’ Rules for Online Safety* by SafeKids.com  
<http://www.safekids.com/kidsrules.htm>  
• Clear list of commitments

*Rules 'N Tools Youth Pledge* by ProtectKids.com

<http://www.protectkids.com/parentsafety/pledge.htm>

- Family Internet safety contract

*Using Family Contracts to Help Protect Your Kids Online* by Microsoft

<http://www.microsoft.com/athome/security/children/famwebrules.msp>

- Sample contract for online code of conduct

*Web Wise Kids: Internet Safety Plan* by WiredWithWisdom

<http://www.wiredwithwisdom.org/internet-safety-plan.pdf>

- Formatted as, "If [blank] happens, I will [blank]"

## Peer to Peer (P2P) or File Sharing

*OnGuard Online: P2P File-Sharing* by Federal Trade Commission

<http://onguardonline.gov/p2p.html>

- Facts and issues involved with *peer-to-peer sharing*

*Sorted: File Sharing* by ChildNet International

<http://www.childnet-int.org/sorted/filessharing.aspx>

- Information on copyright and other legal issues related to *file sharing*

*Young People, Music & the Internet* by ChildNet International

<http://www.childnet-int.org/music/>

- Information and frequently asked questions for parents and young people

## Predators (Including Information on Luring and Grooming)

*How to Recognize "Grooming": Teach Your Kids* by Anne Collier for BlogSafety by Tech Parenting Group

<http://www.blogsafety.com/thread.jspa?threadID=1200000033>

- Tactics and links to other resources

*Online Predators: Help Minimize the Risk* by Microsoft

<http://www.microsoft.com/athome/security/children/kidpred.msp>

- Information on how predators work, tips for parents, and guidelines for children

*Predator Tip Sheet* by i-SAFE

[http://xblock.isafe.org/docs/Eluding\\_Internet\\_Predators\\_Tip\\_Sheet.pdf](http://xblock.isafe.org/docs/Eluding_Internet_Predators_Tip_Sheet.pdf)

- Tips and reminders for recognizing potential problems

## Professional Development

*Every K-12 Professional's Guide to the New Literacies Associated with Information and Communication Technology (ICT) and Higher Student Achievement* by CyberSmart!

<http://www.cybersmart.org/pd/>

[http://www.cybersmart.org/info/overview\\_pres.asp](http://www.cybersmart.org/info/overview_pres.asp)

- Free online course for groups of 25 or more

i-LEARN home page by i-SAFE

<http://ilearn.isafe.org/>

- Free training with online video modules and lesson plans; requires login ID

## Reporting Problems

*Cyberstalking, Cyberbullying and Harassment Report Form* by Wired Safety

<https://www.wiredsafety.org/forms/stalking.html>

- Online form for reporting *cyberstalking* and *cyberbullying*

*CyberTipline* by National Center for Missing & Exploited Children

<http://www.cybertipline.com/>

- Reporting mechanism for child sexual exploitation

*GetNetWise: Reporting Trouble* by Internet Education Foundation

<http://kids.getnetwise.org/trouble/>

- Identifying, reporting, and educating children about online crimes

Internet Crime Complaint Center home page by FBI and National White Collar Crime Center

<http://www.ic3.gov/>

- Mechanism for reporting and investigating online crimes

*OnGuard Online: File a Complaint* by Federal Trade Commission

<http://onguardonline.gov/filecomplaint.html>

- Types of online crimes and who should be notified

*Report a CyberCrime* by ProtectKids.com

<http://www.protectkids.com/report/index.htm>

- Cyber tipline and links to local FBI offices

## Research

*Data Memo* by Amanda Lenhart of Pew Internet and Life Project

<http://www.pewinternet.org/pdfs/PIP%20Cyberbullying%20Memo.pdf>

- A summary of data related to *cyberbullying* collected by Pew

“Internet Prevention Messages: Targeting the Right Online Behaviors” by Michele L. Ybarra, Kimberly J. Mitchell, David Finkelhor, Janis Wolakby in *Pediatrics & Adolescent Medicine*

<http://archpedi.ama-assn.org/cgi/content/abstract/161/2/138>

- Abstract of a study on behaviors that increase risks online (full article requires subscription)
- See Larry Magid’s *blog* entry that summarizes the findings:  
<http://www.blogsafety.com/thread.jspa?threadID=1200000361&tstart=0&mod=1171090729366>

*Just the Facts About Online Youth Victimization: Researchers Present the Facts and Debunk the Myths* (5/3/07)

<http://www.netcaucus.org/events/2007/youth/>

- The nation’s foremost academic researchers on child online safety present their research and answer questions

*Online Victimization: A Report on the Nation’s Youth* (2000) by Center for Missing & Exploited Children

[http://www.missingkids.com/missingkids/servlet/ResourceServlet?LanguageCountry=en\\_US&PageId=869](http://www.missingkids.com/missingkids/servlet/ResourceServlet?LanguageCountry=en_US&PageId=869)

- *Online Victimization of Youth: Five Years Later* (2006) by Center for Missing & Exploited Children  
[http://www.missingkids.com/missingkids/servlet/ResourceServlet?LanguageCountry=en\\_US&PageId=2530](http://www.missingkids.com/missingkids/servlet/ResourceServlet?LanguageCountry=en_US&PageId=2530)
- *Second Youth Internet Safety Survey (YISS-2) Publications* (2007) by Crimes against Children Research Center  
[http://www.unh.edu/ccrc/second\\_youth\\_internet\\_safety-publications.html](http://www.unh.edu/ccrc/second_youth_internet_safety-publications.html)

*Predators vs. Cyberbullies: Reality Check* by Anne Collier for NetFamilyNews.org  
<http://www.safekids.com/2007/03/16/predators-vs-cyberbullies-reality-check/>  
• Examination of the facts presented by Dateline NBC's "To Catch a Predator" and other news shows

*Resources* by Sameer Hinduja and Justin W. Patchin  
<http://www.cyberbullying.us/resources.php>  
• Several research reports conducted by two criminology researchers who specialize in *cyberbullying*

*Safe & Smart: Research and Guidelines for Children's Use of the Internet* by National School Boards Foundation  
<http://www.nsb.org/safe-smart/index.html>  
• Suggestions for using the Internet as a positive force

*Statistics: Online Victimization of Youth: Five Years Later* (2006) by National Center for Missing & Exploited Children (commissioned by Cox Communications)  
<http://www.netismartz.org/safety/statistics.htm>  
• Risks and opportunities of teen Internet use

*Study of Entertainment Media & Health: Internet* by Kaiser Family Foundation  
<http://www.kff.org/entmedia/internet.cfm>  
• Two reports: (1) Internet use by young people in grades 3-12 and (2) online food advertising that targets children

*Technology and Teen Dating Abuse Survey 2007* by Teenage Research Unlimited (TRU) for Liz Claiborne  
[http://www.loveisnotabuse.com/surveyresults\\_2007mstr.htm](http://www.loveisnotabuse.com/surveyresults_2007mstr.htm)  
• Results of a survey on teen dating abuse

*Teens, Privacy and Online Social Networks: How Teens Manage Their Online Identities and Personal Information in the Age of MySpace* by Pew Internet and American Life Project  
[http://www.pewinternet.org/PPF/r/211/report\\_display.asp](http://www.pewinternet.org/PPF/r/211/report_display.asp)  
• Report of surveys conducted by Pew

*What Adults Should Know About Kids' Online Networking* by Kate Sheppard for AlterNet  
<http://www.alternet.org/story/46766/>  
• January 2007 interview with social researcher danah boyd, who focuses on Internet and teens

## Sample School and Division Policies

Andover (Mass.) Public Schools  
[http://www.aps1.net/Internet%20Safety/internet\\_safety.htm](http://www.aps1.net/Internet%20Safety/internet_safety.htm)  
• Internet safety Web page

Dedham (Mass.) Schools  
[http://www.dedham.k12.ma.us/technology/policies/Internet\\_Safety\\_Policy.pdf](http://www.dedham.k12.ma.us/technology/policies/Internet_Safety_Policy.pdf)  
• Internet safety policy, pertaining primarily to *filtering* and *monitoring*

Geneva (Ohio) Area City Schools  
<http://www.genevaschools.org/aup/>  
• Acceptable use and Internet safety policy

Henrico County (Va.) Public Schools  
[http://www.henrico.k12.va.us/pdf/technology/accept\\_use2005.pdf](http://www.henrico.k12.va.us/pdf/technology/accept_use2005.pdf)  
<http://www.henrico.k12.va.us/administration/instruction/technology/safety.html>  
• Acceptable use and Internet safety policy  
• *Internet Safety* Web page

Montgomery County (Md.) Public Schools

<http://www.mcps.k12.md.us/info/cipa/index.shtm>

- *Using the Internet Safely for Educational Purposes* Web page, including links to Internet safety and acceptable use policies

Portland (Maine) Public Schools

<http://www.portlandschools.org/CTS/documents/posterSAUP.pdf>

- Student acceptable use and Internet safety policy

## Sites for Educators

*Bouncing Back: Emergency Planning for IT, Data and Communications Needs* by Vicki Smith Bigham, with contributions from Sheryl Abshire and Mary M. Baker, for the Consortium for School Networking (CoSN)

[http://www.cosn.org/resources/compendium/2007Summaries/BouncingBack\\_emergencyplanning.pdf](http://www.cosn.org/resources/compendium/2007Summaries/BouncingBack_emergencyplanning.pdf)

- Executive summary of a monograph related to IT security, produced and sold by CoSN

*Computer Security Resource Center* by National Institute of Standards and Technology, Computer Security Division

<http://csrc.nist.gov/>

- Resources on security tools and practices

*CSIA Policy Papers* by Cyber Security Industry Alliance

[https://www.csialliance.org/publications/csia\\_whitepapers/](https://www.csialliance.org/publications/csia_whitepapers/)

- Various issues related to *cyber security*, including “Talking Points For Cyber Security”

*Cyberethics for Teachers: A Lesson Plan Outline for Elementary and Middle School Children* by U.S. Department of Justice

<http://www.cybercrime.gov/rules/lessonplan1.htm>

- A lesson defines and explains how to prevent computer crimes

*Cyber Security for the Digital District: Project Overview* by Consortium for School Networking

<http://securedistrict.cosn.org/>

- Security issues superintendents need to know

*Cyber Security for the Digital District: Understanding the Issues: The K-12 Technology Context* by Consortium for School Networking

<http://securedistrict.cosn.org/admin/issue/context.html>

- Far-ranging paper for district superintendents about various security concerns, including student safety

*Educators: A Call to Action: Be a Cyber Secure Student!* by National Cyber Security Alliance

<http://www.staysafeonline.info/basics/educators.html>

- Resources to help students become better cyber citizens

EDUCAUSE CONNECT browse page

[http://www.educause.edu/Browse/645?PARENT\\_ID=702](http://www.educause.edu/Browse/645?PARENT_ID=702)

- Resources on various topics, including *cyber security*, that target primarily higher education but also useful to K-12 administrators

*Help Keep Kids Connected and Protected* by National Cyber Security Alliance

<http://www.staysafeonline.org/connectedandprotected.html>

- Information for educators and parents about *social networking*

*Home Users: A Call to Action: Be a Cyber Secure Citizen!* by National Cyber Security Alliance

<http://www.staysafeonline.info/basics/consumers.html>

- Resources to protect the home from cyber threats

*How to Protect Kids' Privacy Online: A Guide for Teachers* by Federal Trade Commission

<http://www.ftc.gov/bcp/online/pubs/online/teachers.pdf>

- Impact of the federal Children's Online Privacy Protection Act on Web site operators and teachers

*Media Literacy—National Perspective* by the State Education Technology Directors Association (SETDA)

<http://www.setda.org/web/guest/toolkit2007/medialiteracy/nationalperspective>

- A broad overview of media literacy issues, resources, and links

*NetAlert Cybersafe Schools* by Australian Government

[http://www.netalert.gov.au/programs/cybersafe\\_schools.html](http://www.netalert.gov.au/programs/cybersafe_schools.html)

- This excellent guide for schools and teachers about Internet safety includes references to Australian-specific support, but information can be adapted.

*NetAlert: Publications* by Australian Government

<http://www.netalert.gov.au/advice/publications.html>

- Several nicely worded fact sheets for different technologies and safety issues; the references to Australian-specific support can be adapted.

*OnGuard Online: Videos and Tutorials* by Federal Trade Commission

<http://onguardonline.gov/tutorials/index.html>

- Practical tips about cybersecurity

"ONLINE SAFETY: What the Children's Internet Protection Act has in store for you this fall" by Elliott Levine for *Electronic School*, National School Boards Association

<http://www.electronic-school.com/2001/09/0901onlinesafety.html>

- Information about developing an Internet safety policy and using filters

"Out of School Internet Use: A Dilemma for School Officials and Law Enforcement" by Frank Dannahey of the CT Police for WebWiseKids

<http://www.wiredwithwisdom.org/OutofSchoolInternetUse.pdf>

- This report examines legal aspects of Internet safety.

*Play It Cyber Safe: Resources* by Business Software Alliance

<http://www.playitcybersafe.com/resources/index.cfm>

- Resources for teachers and parents

*Safe and Responsible Use of the Internet: A Guide for Educators* by Center for Safe and Responsible Internet Use

<http://csriu.org/onlinedocs/pdf/srui/sruilisting.html>

- Online book covers many issues of concern to educators.

*Safe and Secure?* by Scholastic

<http://content.scholastic.com/browse/article.jsp?id=127>

- Steps for determining network security

*Safe & Smart: Research and Guidelines for Children's Use of the Internet* by National School Boards Foundation

<http://www.nsbf.org/safe-smart/index.html>

- Suggestions for using the Internet as a positive force

*Safeguarding Your Technology* by U.S. Department of Education, National Center for Education Statistics  
<http://nces.ed.gov/pubs98/safetech/>

- Guidelines for administrators to secure computer information, software, and equipment

*Safety and Learning in the Era of Social Networking* by the Consortium for School Networking (CoSN)  
<http://www.cosn.org/resources/compendium/2007Summaries/safetyandlearning.pdf>

- Executive summary of monograph produced and sold by CoSN

*7 Things You Should Know About . . .* by EDUCAUSE  
<http://www.educause.edu/7ThingsYouShouldKnowAboutSeries/7495>

- Series of PDF handouts about various new technologies and their impact on education—geared to higher education but usable for K-12 as well.

US-CERT: U.S. Computer Emergency Readiness Team home page  
<http://www.uscert.gov/>

- Up-to-date information about threats to *cybersecurity*

Virginia Alliance for Secure Computing and Networking home page  
<http://vascan.org/>

- Targeted for Virginia higher-education IT security experts, but also helpful to K-12 IT security officials

*WiredKids: Educators* by WiredKids  
<http://www.wiredkids.org/educators/index.html>

- Articles for educators, including “Internet Problem Issues for Schools” and “Teacher Safety”

## Sites for Kids

Copyright Kids! home page by Copyright Society of the U.S.A.  
<http://www.copyrightkids.org/>

- Information about copyright for students, parents, and children

*Cyberethics for Kids* by U.S. Department of Justice  
<http://www.cybercrime.gov/rules/kidinternet.htm>

- Rules for using the Internet and information about hacking

CyberSpacers home page sponsored by U.S. Department of Justice, Dell, and Information Technology Association of America  
<http://www.cyberspacers.com/>

- Games, comics, and celebrity interviews focusing on cyberethics issues

*Don't Buy It: Get Media Smart* by PBS KIDS  
<http://pbskids.org/dontbuyit/>

- Several interactive learning activities related to media awareness

*FauxPaw the Techno Cat* by iKeepSafe Coalition  
[http://ikeepsafe.org/iksc\\_statemessage/state.php?abbr=VA](http://ikeepsafe.org/iksc_statemessage/state.php?abbr=VA)

- Animated movie and book on the left-side menu relate the adventures of a cat in cyberspace

*Get Your Web License* by PBS KIDS  
<http://pbskids.org/license/>

- Interactive quiz on Internet safety

*GetNetWise: Safety Tips for Kids* by Internet Education Foundation  
<http://kids.getnetwise.org/safetyguide/kids>

- Guidelines for Internet safety

*KidzPrivacy: Just for Kidz* by Federal Trade Commission

<http://www.ftc.gov/bcp/online/edcams/kidzprivacy/kidz.htm>

- Information about surfing, privacy, and personal information

NetSmartzKids home page

<http://www.netsmartzkids.org/indexfl.htm>

- Cartoon characters, games, music videos, and e-cards related to Internet safety

*Notes, Advice and Warnings for Kids on the Web* by The Starport

<http://thestarport.org/Browse/forKids/warn-kids.html>

- Common sense advice for kids in a friendly question-and-answer format

*OnGuard Online: Quizzes* by Federal Trade Commission

<http://onguardonline.gov/quiz/index.html>

- Online quizzes and activities for kids about *identity theft, spyware, phishing, spam*, etc.

*Problem Solver: Stay Safe Online* by National Crime Prevention Council

[http://www.mcgruff.org/Advice/online\\_safety.php](http://www.mcgruff.org/Advice/online_safety.php)

- Rules, pledge, quiz, activities about Internet safety

*Safety Tips: Internet Safety* by FBI Kids

<http://www.fbi.gov/kids/k5th/safety2.htm>

- Concise overview of cyberethics

*Sophia's Safe Surfing Club* by WiredKids

[http://www.wiredkids.org/ktt\\_universal/games/sophia/sophie1.html](http://www.wiredkids.org/ktt_universal/games/sophia/sophie1.html)

- Information and quiz regarding Internet safety, including a printable Internet Safe Surfing Permit

*Surf Swell Island: Adventures in Internet Safety* by Disney

<http://disney.go.com/surfswell/index.html>

- Fun activity site, with many ads

*Web Literacy Tips* by PBS KIDS

<http://pbskids.org/privacy/literacytips.html>

- Concise, simple language kids can understand

*Web Wise Kids: Internet Safety Tips for Kids* by WiredWithWisdom

<http://www.wiredwithwisdom.org/internet-safety-tips-kids.pdf>

- Short list of do's and don't's

## Sites for Older Kids

*Computer Security Awareness Video Contest* by EDUCAUSE

<http://www.educause.edu/SecurityVideoContest/7103>

- Online prize-winning videos by college students

*Don't Believe the Type* by NetSmartz

<http://tcs.cybertipline.com/>

- Links to "Know the Dangers," including tips for keeping safe with various technologies

*GetNetWise: Safety Tips for Teens* by Internet Education Foundation

<http://kids.getnetwise.org/safetyguide/teens>

- Guidelines for online communications

*Internet Superheroes* by WiredKids

<http://www.internetsuperheroes.org/>

- Internet safety/security issues, such as *cyberbullying* and *instant messaging*, using Marvel superheroes

SafeTeens.Com home page by SafeKids.Com and Internet Safety Project

<http://www.safeteens.com/>

- Common sense advice on newer technologies

staysafe.org for Teens home page by staysafe.org

<http://www.msn.staysafeonline.com/teens/default.html>

- Straightforward articles about various technologies and how to enjoy the Internet, stay safe, and communicate with parents

Teenangels home page by WiredSafety

<http://www.teenangels.org/>

- Specially trained teens who spread the word in their schools about Internet safety

*Teen Space* by Identity Theft Resource Center

<http://www.idtheftcenter.org/teen/teen.html>

- A collection of resources for teens about preventing identify theft

*ThinkB4UClick: How to Avoid Doing Something Stupid Online* by Xanga Safety

<http://safety.xanga.com/2006/05/22/thinkb4uclick/>

- Information about netiquette for teens

X-BLOCK: i-MENTORs by i-SAFE

<http://xblock.isafe.org/imentors.php>

- Free online training for students (grades 5-12) to become i-MENTORs and promote Internet safety at school

## Sites for Parents

*Common Sense Internet Safety Guide* by Common Sense Media

<http://www.commonsense.com/download/index.php>

- Free downloadable booklet and weekly e-mail updates

*Don't Believe the Type: For Parents and Guardians* by NetSmartz

<http://tcs.cybertipline.com/parentsguardians.htm>

- Tips for parents to keep their teens safe

*Family & Children: A Call to Action: Be a Cyber Secure Kid!* by National Cyber Security Alliance

<http://www.staysafeonline.info/basics/family.html>

- Resources for parents to protect children

*GetNetWise: Safety Tips for Families* by Internet Education Foundation

<http://kids.getnetwise.org/safetyguide/families>

- Guidelines for protecting children

*Help Keep Kids Connected and Protected* by National Cyber Security Alliance

<http://staysafeonline.org/connectedandprotected.html>

- Guide for educators, parents, and guardians regarding *social networking* sites

*Home Users: A Call to Action: Be a Cyber Secure Citizen!* by National Cyber Security Alliance

<http://www.staysafeonline.info/basics/consumers.html>

- Resources to protect the home from cyber threats

*How to Protect Kids' Privacy Online: A Guide for Teachers* by Federal Trade Commission

<http://www.ftc.gov/bcp/online/pubs/online/kidsprivacy.pdf>

- Impact of the federal Children's Online Privacy Protection Act on Web site operators and parents

*Incredible Internet: Online Safety* by Qwest with the National Center for Missing and Exploited Children

[http://www.incredibleinternet.com/index.php/do/online\\_safety](http://www.incredibleinternet.com/index.php/do/online_safety)

- Useful quiz for parents, plus helpful guides on current safety topics

*Internet Safety: Information for Parents* by WiredKids

<http://www.wiredsafety.org/parent.html>

- Frequently asked questions by parents, including many related to new technologies

*Internet Survival Guide for Parents* by Commonsense Media

<http://www.commonsense.com/internet-safety-guide/>

- Nice information organized by technology type

*i-LEARN Online* by i-SAFE

<http://ilearn.isafe.org/>

- Free online training modules help parents protect their children

*i-SAFE Videos* by OnGuard Online (FTC)

<http://onguardonline.gov/isafevideo.html>

- Clear and concise video for parents about Internet safety (click on "Teach Kids Online Safety" link)

*Keeping Children Safe Online* by U.S. Computer Emergency Response Team

<http://www.us-cert.gov/cas/tips/ST05-002.html>

- Suggestions for parents to protect their children online

*Living with Technology: Keep Your Kids Safe Online* by C/NET (commercial site)

[http://www.cnet.com/2001-13384\\_1-0.html?tag=hed](http://www.cnet.com/2001-13384_1-0.html?tag=hed)

- Several articles highlighting the latest issues, as well as *blog* entries from readers

*Parents* by National Crime Prevention Council

<http://www.ncpc.org/topics/by-audience/parents>

- Overview of dangers and how to protect kids

*A Parent's Guide to Internet Safety* by FBI

<http://www.fbi.gov/publications/pguide/pguidee.htm>

- Detailed publication, including tips and definitions

*A Parent's Guide to Online Kids* by The Children's Partnership

[http://www.childrenspartnership.org/AM/Template.cfm?Section=Speeches\\_and\\_Presentations&CONTENTID=9071&TEMPLATE=/CM/ContentDisplay.cfm](http://www.childrenspartnership.org/AM/Template.cfm?Section=Speeches_and_Presentations&CONTENTID=9071&TEMPLATE=/CM/ContentDisplay.cfm)

- Online PowerPoint presentation covering various types of Internet access and potential benefits/dangers parents should know

*The Parent's Guide to the Information Superhighway: Rules and Tools for Families Online* by The Children's Partnership

[http://www.childrenspartnership.org/AM/Template.cfm?Section=Speeches\\_and\\_Presentations&CONTENTID=4687&TEMPLATE=/CM/HTMLDisplay.cfm](http://www.childrenspartnership.org/AM/Template.cfm?Section=Speeches_and_Presentations&CONTENTID=4687&TEMPLATE=/CM/HTMLDisplay.cfm)

- Downloadable PDF guide, published in 1998 but still provides useful information about children and the Internet

*Parents: Information Overview* by wiredsafety.org

<http://www.wiredsafety.org/parent.html>

- Various briefs on current technology

*Parent's Rules 'N Tools* by ProtectKids.com

<http://www.protectkids.com/parentsafety/index.htm>

- Guidelines for parents in protecting their children

*Resources for Parents* by Family Online Safety Institute

<http://www.fosi.org/resources/parents/>

- Offers a free parental control bar for helping *filter* sites when children use the Internet

*Resources for Parents* by WebWiseKids

[http://www.wiredwithwisdom.org/parent\\_resources.asp](http://www.wiredwithwisdom.org/parent_resources.asp)

- Links to Internet safety Web sites

Safe Surfin' Foundation home page by safesurfincentral.org

<http://www.safesurfincentral.org/>

- Resources on educating young people about Internet crimes

*Social Networking Sites: A Parent's Guide* by Federal Trade Commission

<http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec13.pdf>

- Tips for protecting children

*10 Common Questions about Internet Safety* by iKeepSafe.org and Symantec

[http://www.ikeepsafe.org/iksc\\_partners/symantec/](http://www.ikeepsafe.org/iksc_partners/symantec/)

- Free online "Parent's Tech Tutorial"

*Teach Your Kids to Protect Their Online Reputations* by staysafe.org for Parents

<http://www.msn.staysafeonline.com/parents/default.html>

- Articles explaining newer technologies, communication and safety issues, and practical tips for using software to keep children safe

*Web Wise Kids: Tips for Parents* by WiredWithWisdom

<http://www.wiredwithwisdom.org/internet-safety-tips-parents.pdf>

- List of recommendations for parents

*What Parents Can Do About Internet Safety* by Larry Magid for Safekids.com

[http://www.safekids.com/articles/parents\\_can.htm](http://www.safekids.com/articles/parents_can.htm)

- Short article citing recent statistics (published 11/06)

*WiredKids: Parents* by WiredKids

<http://www.wiredkids.org/parents/index.html>

- Resources available under "Parent" pull-down menu

## Social Networking (Blogs, Personal Web Pages, Chats)

*Blogsafety* by Childnet International

<http://www.childnet-int.org/blogsafety/>

- Excellent site with advice for all stakeholders

*ChatDanger: How to Keep SAFE While Chatting Online* by Childnet International

<http://www.chatdanger.com/>

- *Social networking* true stories

*ConnectSafely Forum* by Tech Parenting Group

<http://www.blogsafety.com/>

- Information for kids, parents, and teachers about how to use *blogs* safely, including acronyms

*GetNetWise: Chat* by Internet Education Foundation

<http://kids.getnetwise.org/safetyguide/technology/chat>

- Suggestions for avoiding problems in *chat rooms*

*GetNetWise: Social Networking Sites* by Internet Education Foundation

<http://kids.getnetwise.org/safetyguide/technology/socialnetworking>

- Suggestions for parents and children

*A Guide to MySpace for Parents with Teens* by MySpace

<http://creative.myspace.com/safety/safetyguideparents.pdf>

- Guide to using MySpace safely, sponsored by MySpace and *Seventeen* magazine

*Safety Tips* by MySpace

<http://www1.myspace.com/misc/tipsForParents.html>

- Safety Tips posted on the MySpace Web site

*Safety Tips for Chat Rooms* by Microsoft

<http://www.microsoft.com/athome/security/online/chatsafety.msp>

- Recommendations for both parents and kids

*7 Things You Should Know About Virtual Worlds* by EDUCAUSE

<http://www.educause.edu/LibraryDetailPage/666?ID=ELI7015>

- PDF handout covering the basics on virtual worlds and their use in higher education

*7 Things You Should Know about Wikis* by EDUCAUSE

<http://www.educause.edu/LibraryDetailPage/666?ID=ELI7004>

- PDF handout covering the basics on Wikis and their use in higher education

*Social Networking and DOPA* by the Young Adult Library Services Association

[http://www.leonline.com/yalsa/positive\\_uses.pdf](http://www.leonline.com/yalsa/positive_uses.pdf)

- Overview of *social networking*, including positive uses for education

*Social Networking Sites: Safety Tips for Tweens and Teens* by Federal Trade Commission

<http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec14.pdf>

- Tips for socializing safely online

2 SMRT 4U home page by The National Center for Missing & Exploited Children

<http://www.2smrt4u.com/>

- *Social networking* safety site specifically designed for young girls

*A Word on Safety* by YouTube

<http://www.youtube.com/t/safety>

- A brief explanation of how to stay safe if posting videos on YouTube

### Safe Social Networking Sites for Younger Kids

Club Penguin home page (some parts require fees)

<http://clubpenguin.com/>

Imbee.com home page

<https://www.imbee.com/>

Whyville home page

<http://www.whyville.net/smmk/nice>

### Student Instruction: Lesson Plans/Curricula

*Activities and Lessons* by Wired Safety

<http://www.wiredsafety.org/wiredlearning/toc.html>

- Features great lessons

*Curriculum Scope* by CyberSmart Education Company

[http://www.cybersmartcurriculum.org/curr\\_over/](http://www.cybersmartcurriculum.org/curr_over/)

- 65 lesson plans, arranged by age level and subtopic (safety, manners, advertising, research, and technology), with individual lessons (under “Lesson Plans and Activity Sheets”) and posters, sample letters to parents, and tips for home Internet use (under “More Free Stuff”)

*Cyberethics for Teachers: A Lesson Plan Outline for Elementary and Middle School Children* by U.S.

Department of Justice

<http://www.cybercrime.gov/rules/lessonplan1.htm>

- Lesson plan that defines and explains how to prevent computer crimes

*Digital Ethics* by Nortel LearnIT

[http://www.nortellearnit.org/LearnIT/technology/Digital\\_Ethics/](http://www.nortellearnit.org/LearnIT/technology/Digital_Ethics/)

- Links to short informational videos about Internet ethics

*Educational Games* by Media Awareness Network

<http://www.media-awareness.ca/english/games/index.cfm>

- Interactive games with teacher’s guides for educating about Internet safety, advertising ploys, and hate sites

*Educators* by NetSmartz

<http://www.netsmartz.org/educators.htm>

- Classroom materials that teach children to be safe online

*iLEARN Online* by i-SAFE

<http://ilearn.isafe.org/>

- Curriculum available only after online training

*Media Awareness—How Media Savvy Are You?* by M. Velthuzien, American School of the Hague librarian

<http://fc.ash.nl/~mvelthuizen/FOV2-0000E021/S0011C50C?Plugin=Block>

- Links for teachers to use when teaching students to be media savvy

*Online Safety* by Nortel LearnIT

[http://www.nortellearnit.org/LearnIT/technology/Online\\_Safety/](http://www.nortellearnit.org/LearnIT/technology/Online_Safety/)

- Links to short informational videos about Internet safety

*Resources/WWK Videos* by WebWiseKids

<http://www.webwisekids.org/index.asp?page=videos>

- These interactive video resources are free to Virginia's schools.

*Safe Passage: Introduction* by Media Awareness Network

[http://www.media-awareness.ca/english/teachers/wa\\_teachers/safe\\_passage\\_teachers/index.cfm](http://www.media-awareness.ca/english/teachers/wa_teachers/safe_passage_teachers/index.cfm)

- Links to Internet safety topics with lesson plans

## Wireless

*GetNetWise: Spotlight on Wireless Security* by GetNetWise

<http://spotlight.getnetwise.org/wireless/>

- Information on keeping your wireless network safe and secure



## Appendix E

### Glossary

**blog/blogging:** This term is derived from *Web log* and is an increasingly popular type of Web site. Most take the form of journal entries and allow readers to post comments.

**bookmark(s):** This browser feature stores a Web address in memory and allows the user to link quickly to the site.

**chat rooms:** These Web sites or online services facilitate electronic discussions by quickly posting the comments and responses of multiple users.

**circumventor sites:** These parallel Web sites allow children to get around some *filtering* software and access sites that have been blocked.

**cyberbullies/cyberbullying:** This refers to any online threats by one student toward another, typically through e-mails or on Web sites (e.g., *blogs*, *social networking* sites).

**cybercrime:** This refers to any Internet-related illegal activity.

**cybersecurity (sometimes *cyber security*):** This refers to any technique, software, etc., used to protect computers and prevent online crime.

**cyberstalking:** This refers to a number of methods individuals use to track, lure, or harass another person online.

**electronic footprints:** Computers maintain a record of all Web site visits and e-mail messages, leaving a trail of the user's activity in cyberspace. These data can still exist even after the browser *history* has been cleared and e-mail messages have been deleted.

**favorite(s):** This is the name for *bookmarks* (see above) used by Microsoft's Internet Explorer browser.

**file sharing:** This software enables multiple users to access the same computer file simultaneously. File sharing sometimes is used illegally to download music or software.

**filter/filtering:** This refers to different types of software that screen and block online content.

**gaming:** This term describes Internet games, which can be played either individually or by multiple online users at the same time.

**griefers:** These Internet users intentionally cause problems for other *gamers*.

**grooming:** This refers to the techniques sexual predators use to get to know their victims in preparation for sexual abuse.

**history:** This is a tracking feature of Internet browsers that shows all the recent Web sites visited.

**identity theft:** In this crime, someone obtains the vital information (e.g., credit card, Social Security, bank account numbers) of another person, usually to steal money. E-mail scams, *spyware*, and *viruses* are among the most typical methods for stealing someone's identity.

**instant message/messaging:** Known by the acronym *IM*, this is a variation of *chat rooms* that allows users to communicate through text messages.

**malicious code:** This refers to any computer code that is intentionally introduced into a system to damage or destroy files or disrupt the operation of a computer.

**monitoring:** This refers generally to the technique of tracking where people have been on the Internet by looking at the *history* of the browser. It also refers to software used for the same purpose.

**P2P (see peer-to-peer computing)**

**peer-to-peer (P2P) computing:** This is a popular way for Internet users to share one another's computer files—usually music, game, or software files.

**phishing:** This scam involves sending a fraudulent e-mail soliciting credit card, Social Security, or other personal information from an unsuspecting user.

**social networking:** This refers broadly to online communities where people share information about themselves, music files, photos, etc. There are many social networking Web sites (e.g., MySpace, Facebook, or Friendster).

**spam:** This refers to any unsolicited e-mail, or junk mail. Most spam is either a money scam or sexual in nature. Internet Service Providers, e-mail software, and other software can help block some, but not all, spam.

**spyware:** This refers to a wide-variety of software installed on people's computers without their knowledge. The programs typically will track computer use and create numerous pop-up ads. In some instances, the spyware can damage the computer and facilitate *identity theft*.

**viruses:** These are software programs that typically arrive through e-mail attachments and multiply on the hard drive, quickly exhausting the computer's memory. A *trojan* is a variation that allows unauthorized users access to the computer, from which they can send infected e-mails or *spam*.

**wireless computers:** Many networks now allow computers access to the Internet without being connected with wires. These networks are becoming increasingly more popular and powerful, allowing people to access the Internet using cell phones and other devices.



## NOTES

[illegible]





## NOTES

[illegible]





<http://www.doe.virginia.gov/VDOE/Technology/OET/internet-safety-guidelines.shtml>

---

The Virginia Department of Education does not unlawfully discriminate on the basis of sex, race, color, religion, disabilities, or national origin in employment or in its educational programs and activities.